Polar codes for private classical communication

Mark M. Wilde
School of Computer Science, McGill University
Montreal, Quebec, Canada

Joseph M. Renes
Institut für Theoretische Physik, ETH Zurich
Zürich, Switzerland

***Abstract*—We construct a new secret-key assisted polar coding scheme for private classical communication over a quantum or classical wiretap channel. The security of our scheme rests on an entropic uncertainty relation, in addition to the channel polarization effect. Our scheme achieves the symmetric private information rate by synthesizing "amplitude" and "phase" channels from an arbitrary quantum wiretap channel. We find that the secret-key consumption rate of the scheme vanishes for an arbitrary degradable quantum wiretap channel. Furthermore, we provide an additional sufficient condition for when the secret key rate vanishes, and we suspect that satisfying this condition implies that the scheme requires no secret key at all. Thus, this latter condition addresses an open question from the Mahdavifar-Vardy scheme [1] for polar coding over a classical wiretap channel.**

Polar coding is one of the most exciting recent developments in coding and information theory [2]. The codes are based on the *channel polarization* effect and are provably capacity-achieving with an $O\left(N \log N\right)$ complexity for both encoding and decoding, where N is the number of channel uses.

Several researchers have now extended the polar coding method to a variety of scenarios, one of which includes the secure transmission of classical data over a wiretap channel [1]. The polar codes constructed in Ref. [1] meet a "strong security" criterion, which requires that the mutual information between the sender's information bits and the wiretapper's channel outputs decrease to zero as $N \rightarrow \infty$. Guha and Wilde later exploited the ideas from Refs. [1], [3] to construct polar codes for private data transmission over a quantum wiretap channel [4], and the resulting codes achieve the symmetric private information rate whenever the channel to the wiretapper is classical.

An important question left open from Ref. [1] is to determine if it is possible for the Mahdavifar-Vardy polar coding scheme to be both reliable and strongly secure. Ref. [4] made partial progress on this question by suggesting a simple solution: just allow for the sender and receiver to share some secret key before communication begins. In spite of its simplicity, this solution is undesirable from a practical perspective because it might be difficult for the sender and receiver to establish good secret key in the first place. Though, Proposition 22 in Ref. [1] proves that the rate of secret key needed vanishes if the wiretap channel is degradable.

In this paper, we construct a new polar coding scheme for private classical communication over a quantum wiretap channel. As classical wiretap channels are special cases of quantum wiretap channels, all of our results here apply to them as well. The security of our scheme has a physical basis, due to an entropic uncertainty relation [5]. In fact, our scheme is secure in the strongest information-theoretic sense, against a wiretapper who has access to unbounded quantum computational power. The new scheme offers several improvements over the schemes from Refs. [1], [4]:

- The net rate of private classical communication is equal to symmetric private information for an *arbitrary* quantum channel with qubit input.
- The secret key consumption rate vanishes for an *arbitrary* degradable quantum wiretap channel.
- We provide an additional sufficient condition for when the secret key rate of our polar coding scheme vanishes (it is based on that in Ref. [6]—we suspect that satisfying this condition means the code does not require any secret key bits at all). Since our results here apply to classical wiretap channels as well, this result addresses the open question from Ref. [1]. We show that the condition is satisfied for some example channels (including the one from Ref. [1]) for a wide range of interesting parameters.

We begin in the next section with some notation and definitions. Section II overviews our private polar coding scheme and proves that it is both reliable and secure if sufficient secret key is available. Section III proves that the rate of secret key vanishes if the quantum wiretap channel is degradable, and the same section provides an additional sufficient condition for when the secret key rate of the polar coding scheme vanishes. Finally, we conclude in Section IV with a summary.

I. Notation and Definitions

A binary-input *classical-quantum* (cq) channel $W : x \rightarrow \rho_x$ prepares a quantum state ρ_x at the output, depending on an input classical bit x. Two parameters that determine the performance of W are the fidelity $F\left(W\right) \equiv \left\| \sqrt{\rho_0}\sqrt{\rho_1} \right\|_1^2$ and the symmetric Holevo information $I\left(W\right) \equiv H\left(\left(\rho_0 + \rho_1\right)/2\right) - \left[H\left(\rho_0\right) + H\left(\rho_1\right)\right]/2$ where $H\left(\sigma\right) \equiv -\text{Tr}\{\sigma \log_2 \sigma\}$ is the von Neumann entropy. These parameters generalize the Bhattacharya parameter and the symmetric mutual information [2], respectively, and are related as $I\left(W\right) \approx 1 \Leftrightarrow F\left(W\right) \approx 0$ and $I\left(W\right) \approx 0 \Leftrightarrow F\left(W\right) \approx 1$ [3]. The channel W is near perfect when $I\left(W\right) \approx 1$ and near useless when $I\left(W\right) \approx 0$.

II. Private Polar Coding Scheme

A. Classical-quantum channels for complementary variables

Consider a quantum wiretap channel $\mathcal{N}^{A' \rightarrow BE}$ [7], [8] with a qubit input system A' for the sender Alice, an output system B for the legitimate receiver Bob, and an output

system E for the wiretapper Eve. The channel $\mathcal{N}^{A'\to B}$ from the sender to the legitimate receiver arises by tracing over the wiretapper's system: $\mathcal{N}^{A'\to B}(\rho) \equiv \text{Tr}_E\{\mathcal{N}^{A'\to BE}(\rho)\}$, where ρ is some qubit input to the channel. Let $U_{\mathcal{N}}^{A'\to BES_2}$ denote an isometric extension of this channel [9], such that S_2 is its environment. The system S_2 is known as a "shield" system [10], [11], which is not available to the wiretapper and may or may not be available to the legitimate receiver. The security of our scheme is in part based on the fact that this shield system is not available to the wiretapper.

This quantum wiretap channel $\mathcal{N}^{A'\to BE}$ captures the case in which the wiretapper has access to all the physical degrees of freedom that are not available to the legitimate receiver (so that S_2 is a trivial system in this case). It also captures the more specialized case in which the output systems B and E are classical systems (as in the classical wiretap channel [12]). (See Appendix A for a brief discussion of this latter point.)

Following Ref. [13], we can produce a protocol for sending classical information privately over the quantum wiretap channel $\mathcal{N}^{A'\to BE}$ by considering two different complementary channels arising from it. Both of these derived channels are cq channels that have a classical input bit and a quantum output depending on this input bit.

The first channel that we consider has Alice prepare a quantum state $\rho_z^{A'}$ depending on the value of an input bit z. She then feeds this state into the channel $\mathcal{N}^{A'\to B}$:

$$W_{A,B} : z \to \mathcal{N}^{A'\to B}(\rho_z^{A'}). \tag{1}$$

We call the above channel the "amplitude cq channel," and the notation $W_{A,B}$ indicates that it is an amplitude (A) channel to Bob (B). The state $\rho_z^{A'}$ can generally be a mixed state, as would arise, for instance, from using randomness at the encoder. It thus admits a *purification* $|\psi_z\rangle^{A'S_1}$, which is some pure state on a larger tensor-product Hilbert space $\mathcal{H}^{A'} \otimes \mathcal{H}^{S_1}$ such that tracing over the purifying system S_1 gives back the original state: $\rho_z^{A'} = \text{Tr}_{S_1}\{|\psi_z\rangle\langle\psi_z|^{A'S_1}\}$. The system S_1 is an additional shield system because it represents another system that is not available to the wiretapper (though in this case, Alice always has access to this shield system). By purifying all systems, we can see that the amplitude channel in (1) arises by tracing over the S_1S_2E systems of the following cq channel:

$$z \to |\psi_z\rangle^{BES_1S_2} \equiv U_{\mathcal{N}}^{A'\to BES_2} |\psi_z\rangle^{A'S_1}. \tag{2}$$

The symmetric Holevo information of this amplitude channel $W_{A,B}$ is equal to $I(W_{A,B}) \equiv I(Z;B)_\xi$, where the mutual information $I(Z;B)$ is computed with respect to

$$\xi^{ZBE} \equiv \frac{1}{2}\sum_z |z\rangle\langle z|^Z \otimes \mathcal{N}^{A'\to BE}(\rho_z^{A'}). \tag{3}$$

The second cq channel that we consider is a phase channel with quantum side information (QSI). Suppose now that Alice has access to an entangled state of the following form:

$$|\varphi\rangle^{CA'S_1} \equiv \frac{1}{\sqrt{2}}\sum_z |z\rangle^C |\psi_z\rangle^{A'S_1}. \tag{4}$$

If so, Alice could then modulate the C system by applying a phase operator Z^x to it, depending on some bit x. If she is then able to transmit the A' system through the channel $\mathcal{N}^{A'\to B}$ and the C and S_1 systems through an identity channel, the resulting channel to Bob is as follows:

$$W_{P,B} : x \to \omega_x^{BCS_1S_2}, \tag{5}$$
$$\omega_x^{BCS_1S_2} \equiv \text{Tr}_E\{U_{\mathcal{N}}^{A'\to BES_1}[(Z^x)^C |\varphi\rangle\langle\varphi|^{CA'S_1} (Z^x)^C]\}.$$

The notation $W_{P,B}$ indicates that this is a phase (P) channel to Bob (B). By including the wiretapper E as well, the channel acts as follows (where we should subsequently trace over E):

$$\begin{aligned} x &\to (Z^x)^C U_{\mathcal{N}}^{A'\to BES_2} |\varphi\rangle^{CA'S_1} \\ &= \frac{1}{\sqrt{2}}\sum_z (-1)^{xz} |z\rangle^C |\psi_z\rangle^{BES_1S_2}. \end{aligned} \tag{6}$$

The symmetric Holevo information of this amplitude channel $W_{P,B}$ is equal to $I(W_{P,B}) \equiv I(X;BCS_1S_2)_\eta$, where the mutual information is computed using the following state:

$$\eta^{XBCS_1S_2} \equiv \frac{1}{2}\sum_x |x\rangle\langle x|^X \otimes \omega_x^{BCS_1S_2}. \tag{7}$$

Although it is not immediately obvious, the phase channel $W_{P,B}$ is useful in constructing polar codes for private classical communication. Its importance stems from the fact that it is intimately related to the amplitude channel from the sender to the wiretapper Eve, via an uncertainty relation [5]. Indeed, consider the channel from Alice's input bit z to the wiretapper:

$$W_{A,E} : z \to \mathcal{N}^{A'\to E}(\rho_z^{A'}), \tag{8}$$

where $\mathcal{N}^{A'\to E}$ is the channel that results from tracing over Bob's system after applying the wiretap channel $\mathcal{N}^{A'\to BE}$. The notation $W_{A,E}$ indicates that this channel is an amplitude (A) channel to Eve (E). The symmetric Holevo information of this channel is equal to $I(W_{A,E}) \equiv I(Z;E)_\xi$.

The important uncertainty relation between the channels $W_{P,B}$ and $W_{A,E}$ is then as follows:

$$I(W_{P,B}) + I(W_{A,E}) = 1, \tag{9}$$

which is a special case of Lemma 2 from Ref. [13]. We interpret the above uncertainty relation as "*if the phase channel to Bob is nearly perfect, then the amplitude channel to Eve must be nearly useless and vice versa*."

The above uncertainty relation then enables us to construct a reliable and strongly secure polar coding scheme for sending private classical data. As outlined in Section II-C our scheme has the sender transmit private information bits through the synthesized channels (in the polar coding sense) that are nearly perfect in both amplitude and phase for Bob. The fact that these synthesized amplitude channels are nearly perfect guarantees that Bob will be able to recover these bits reliably, and that these synthesized phase channels are nearly perfect for Bob guarantees that Eve will be able to recover only a negligibly small amount of information about the bits sent through them, due to the above uncertainty relation.

Partitioning the synthesized channels according to amplitude and phase for Bob, rather than according to amplitude for Bob and amplitude for Eve as in Refs. [1], [4], has the advantage that the scheme achieves the symmetric private information rate for all quantum wiretap channels. Moreover, we can prove that the secret key consumption rate vanishes for all degradable quantum channels, and we can furthermore provide an additional sufficient condition for when the secret key rate of the polar coding scheme vanishes.

B. Channel Polarization

Ref. [3] demonstrated how to construct synthesized versions of W, by channel combining and splitting [2]. The synthesized channels $W_N^{(i)}$ are of the following form:

$$W_N^{(i)} : u_i \to \rho_{(i),u_i}^{U_1^{i-1}B^N}, \tag{10}$$

$$\rho_{(i),u_i}^{U_1^{i-1}B^N} \equiv \sum_{u_1^{i-1}} \frac{1}{2^{i-1}} \left|u_1^{i-1}\right\rangle \left\langle u_1^{i-1}\right|^{U_1^{i-1}} \otimes \overline{\rho}_{u_1^i}^{B^N}, \tag{11}$$

$$\overline{\rho}_{u_1^i}^{B^N} \equiv \sum_{u_{i+1}^N} \frac{1}{2^{N-i}} \rho_{u^N G_N}^{B^N}, \qquad \rho_{x^N}^{B^N} \equiv \rho_{x_1}^{B_1} \otimes \cdots \otimes \rho_{x_N}^{B_N},$$

where G_N is Arikan's encoding circuit matrix built from classical CNOT and permutation gates. If the channel is classical, then these states are diagonal in the computational basis, and the above states correspond to the distributions for the synthesized channels [2]. The interpretation of $W_N^{(i)}$ is that it is the channel "seen" by the input u_i if the previous bits u_1^{i-1} are available and if the future bits u_{i+1}^N are randomized. This motivates the development of a quantum successive cancellation decoder [3] that attempts to distinguish $u_i = 0$ from $u_i = 1$ by adaptively exploiting the results of previous measurements and quantum hypothesis tests for each bit decision.

The synthesized channels $W_N^{(i)}$ polarize, in the sense that some become nearly perfect for classical data transmission while others become nearly useless. To prove this result, one can model the channel splitting and combining process as a random birth process [2], [3], and one can demonstrate that the induced random birth processes corresponding to the channel parameters $I(W_N^{(i)})$ and $F(W_N^{(i)})$ are martingales that converge almost surely to zero-one valued random variables in the limit of many recursions. The following theorem characterizes the rate with which the channel polarization effect takes hold [14], [3], and it is useful in proving statements about the performance of polar codes for cq channels:

Theorem 1: Given a binary input cq channel W and any $\beta < 1/2$, it holds that $\lim_{n\to\infty} \Pr_I\{\sqrt{F(W_{2^n}^{(I)})} < 2^{-2^{n\beta}}\} = I(W)$, where n indicates the level of recursion for the encoding, $W_{2^n}^{(I)}$ is a random variable characterizing the I^{th} split channel, and $F(W_{2^n}^{(I)})$ is the fidelity of that channel.

Assuming knowledge of the good and bad channels, one can then construct a coding scheme based on the channel polarization effect, by dividing the synthesized channels according to the following polar coding rule:

$$\mathcal{G}_N(W,\beta) \equiv \left\{i \in [N] : \sqrt{F(W_N^{(i)})} < 2^{-N^\beta}\right\}, \tag{12}$$

and $\mathcal{B}_N(W,\beta) \equiv [N] \setminus \mathcal{G}_N(W,\beta)$, so that $\mathcal{G}_N(W,\beta)$ is the set of "good" channels and $\mathcal{B}_N(W,\beta)$ is the set of "bad" channels. The sender then transmits the information bits through the good channels and "frozen" bits through the bad ones. A helpful assumption for error analysis is that the frozen bits are chosen uniformly at random such that the sender and receiver both have access to these frozen bits. Ref. [3] provided an explicit construction of a quantum successive cancellation decoder that has an error probability equal to $o(2^{-N^\beta})$—let $\{\Lambda_{u_{\mathcal{A}}}^{(u_{\mathcal{A}^c})}\}$ denote the corresponding decoding positive operator-valued measure (POVM) [9], with $u_{\mathcal{A}}$ the information bits and $u_{\mathcal{A}^c}$ the frozen bits.

For our polar coding scheme for private communication, we can imagine that the classical bits fed into the encoder are encoded into the classical states $|0\rangle$ and $|1\rangle$ and that the encoder is a coherent, quantum version of Arikan's encoder [2], meaning that the gates are quantum CNOTs and permutations (i.e., the same encoder as in Refs. [6], [4]). This perspective is helpful in our subsequent analysis of the phase channels, though it need not be the case in practice—the scheme will work perfectly well if the bits are just classical bits and the encoder is Arikan's classical encoder. When sending amplitude-basis classical information through the encoder and channels, the effect is to induce synthesized channels $W_{A,N}^{(i)}$ as described above. Theorem 1 states that the fraction of amplitude-good channels (according to the criterion in (12)) is equal to $I(Z;B)_\xi$.

We now consider how the encoder induces synthesized channels for the phase-basis classical information. It is important to keep in mind for our development in this paper that these channels are merely virtual—we just consider them in order to relate back to the amplitude channels to Eve via an uncertainty relation (this uncertainty relation will be a slightly modified version of that in (9)). The benefit of this approach is that we can broaden the results of Refs. [1], [4] and make sharper statements about the code's secret key consumption.

Proceeding similarly to Ref. [6], [15], the same encoding operation leads to channel polarization for the phase channel $W_{P,B}$ as well. Suppose Alice modulates her halves of the entangled pairs as in the definition of W_P, but then inputs them to the coherent encoder before sending them via the channel to Bob. The result is

$$\frac{1}{\sqrt{2^N}} \sum_{z^N \in \{0,1\}^N} (-1)^{x^N \cdot z^N} \left|\psi_{z^N G_N}\right\rangle^{B^N E^N S_1^N S_2^N} \left|z^N\right\rangle^{C^N},$$

whose $B^N S_1^N S_2^N C^N$ marginal state is simply $U_{\mathcal{E}}^{C^N} \omega_{x^N G_N^T}^{B^N S_1^N S_2^N C^N} U_{\mathcal{E}}^{\dagger C^N}$, where $U_{\mathcal{E}}$ denotes the polar encoder. Here we have used the fact that the matrix corresponding to G_N is invertible. Thus, the coherent encoder also induces synthesized channels $W_{P,N}^{(i)}$ using the encoding matrix G_N^T instead of G_N, modulo the additional $U_{\mathcal{E}}$ acting on C^N. Theorem 1 states that the fraction of phase-good

channels to Bob (according to the criterion in (12)) is approximately equal to $I\left(X;BCS_1S_2\right)_\eta$.

Note that the classical side information for the $W_{P,N}^{(i)}$ is different from that in (10) because the direction of all CNOT gates is flipped due to the transpose of G_N when acting on phase variables. This means means that the i^{th} synthesized phase channel $W_{P,N}^{(i)}$ is such that all of the *future* bits $x_N \cdots x_{i+1}$ are available to help in decoding bit x_i while all of the *previous* bits $x_{i-1} \cdots x_1$ are randomized. (This is the same as described in Ref. [6] for Pauli channels.)

A clear advantage of the current approach over the previous construction from Ref. [4] is that Theorem 1 directly applies to the phase-good channels with the "goodness criterion" given by (12). Ref. [4] considered the amplitude channels to Eve (rather than the phase-good channels to Bob), and it seemed only possible to prove polarization results for quantum wiretap channels in which the amplitude channel to Eve is classical. Our approach here overcomes this difficulty by appealing to Theorem 1 directly for polarization and later relating the phase channels to Bob and the amplitude channels to Eve via an uncertainty relation (similar to the approach from Ref. [15]).

C. Private Polar Coding Scheme

We can now specify our polar coding scheme. Divide the synthesized cq amplitude channels $W_{A,B,N}^{(i)}$ into sets $\mathcal{G}_N\left(W_{A,B},\beta\right)$ and $\mathcal{B}_N\left(W_{A,B},\beta\right)$ according to (12), and similarly, divide the synthesized cq phase channels $W_{P,B,N}^{(i)}$ into sets $\mathcal{G}_N\left(W_{P,B},\beta\right)$ and $\mathcal{B}_N\left(W_{P,B},\beta\right)$, where $\beta < 1/2$. The synthesized channels correspond to particular inputs to the encoding operation, and thus the set of all inputs divides into four groups: those that are good for both the amplitude and phase variable, those that are good for amplitude and bad for phase, bad for amplitude and good for phase, and those that are bad for both variables. We denote these channels as follows:

$$\begin{aligned}
\mathcal{A} &\equiv \mathcal{G}_N\left(W_{A,B},\beta\right) \cap \mathcal{G}_N\left(W_{P,B},\beta\right),\\
\mathcal{X} &\equiv \mathcal{G}_N\left(W_{A,B},\beta\right) \cap \mathcal{B}_N\left(W_{P,B},\beta\right),\\
\mathcal{Z} &\equiv \mathcal{B}_N\left(W_{A,B},\beta\right) \cap \mathcal{G}_N\left(W_{P,B},\beta\right),\\
\mathcal{B} &\equiv \mathcal{B}_N\left(W_{A,B},\beta\right) \cap \mathcal{B}_N\left(W_{P,B},\beta\right).
\end{aligned}$$

Our polar coding scheme for private classical communication has the sender transmit information bits through the inputs in $\mathcal{A}$, random bits through the inputs in $\mathcal{X}$, frozen bits through the inputs in $\mathcal{Z}$, and halves of secret key bits through the inputs in $\mathcal{B}$. It is straightforward to prove that the net rate of private classical communication $\left(|\mathcal{A}| - |\mathcal{B}|\right)/N$ is equal to the symmetric private information $I\left(Z;B\right)_\xi - I\left(Z;E\right)_\xi$ by observing that the fraction of amplitude-good channels is $I\left(Z;B\right)_\xi$, the fraction of phase-good channels is $I\left(X;BCS_1S_2\right)_\eta$, and exploiting the uncertainty relation $I\left(X;BCS_1S_2\right)_\eta = 1 - I\left(Z;E\right)_\xi$ from (9). A detailed proof is similar to the proof given in Appendix A of Ref. [15].

We should stress that our consideration of the phase channels in this paper is only necessary in order to compute the index sets $\mathcal{A}$, $\mathcal{X}$, $\mathcal{Z}$, and $\mathcal{B}$. The decoder in the next section does not make explicit use of these phase channels—they only arise in our security analysis, where we appeal to an entropic uncertainty relation in order to guarantee security of the scheme. This is in contrast to our polar coding scheme for sending *quantum* information [15], in which the decoder makes explicit use of the phase channels.

D. Reliability and Security Analysis

First, it is straightforward to prove that the code has good reliability, by appealing to the results from Ref. [3]. That is, there exists a POVM $\{\Lambda_{u_\mathcal{A},u_\mathcal{X}}^{(u_\mathcal{B})}\}$ such that

$$\Pr\{\widehat{U}_\mathcal{C} \neq U_\mathcal{C}\} \leq \sqrt{2\sum_{i\in\mathcal{C}}\sqrt{F(W_{A,B,N}^{(i)})}} = o\left(2^{-\frac{1}{2}N^\beta}\right).$$

where $\mathcal{C} \equiv \mathcal{A}\cup\mathcal{X}$. This POVM is the quantum successive cancellation decoder established in Ref. [3]. The quantum successive cancellation decoder operates exactly as before, but it needs to decode both the information bits in $\mathcal{A}$ and the randomized bits in $\mathcal{X}$. It also exploits the frozen bits in $\mathcal{Z}$ and the secret key bits in $\mathcal{B}$ to help with decoding. This decoder has an efficient implementation if the channel to Bob is classical [2]. This is the case for the amplitude damping channel and any Pauli channel, for example.

We now prove that strong security, in the sense of Ref. [1], holds for our polar coding scheme.

Theorem 2: For sufficiently large N, the private polar coding scheme given above satisfies the following strong security criterion: $I\left(U_\mathcal{A};E^N\right) = o(2^{-\frac{1}{2}N^\beta})$.

Proof: Consider that

$$\begin{aligned}
I\left(U_\mathcal{A};E^N\right) &= \sum_{i\in\mathcal{A}} I\left(U_i;E^N|U_{\mathcal{A}_i^-}\right) = \sum_{i\in\mathcal{A}} I\left(U_i;E^N U_{\mathcal{A}_i^-}\right)\\
&\leq \sum_{i\in\mathcal{A}} I\left(U_i;E^N U_1^{i-1}\right) = \sum_{i\in\mathcal{A}} I(W_{A,E,N}^{(i)})
\end{aligned}$$

The first equality is from the chain rule for quantum mutual information and by defining $\mathcal{A}_i^-$ to be the indices in $\mathcal{A}$ preceding i. The second equality follows from the assumption that the bits in $U_{\mathcal{A}_i^-}$ are chosen uniformly at random. The first inequality is from quantum data processing. The third equality is from the definition of the synthesized channels $W_{A,E,N}^{(i)}$. Continuing, we have

$$\begin{aligned}
&\leq \sum_{i\in\mathcal{A}} \sqrt{1 - F(W_{A,E,N}^{(i)})} \leq \sum_{i\in\mathcal{A}} \sqrt{1 - (1 - 2F(W_{P,B,N}^{(i)})^{\frac{1}{2}})^2}\\
&\leq \sum_{i\in\mathcal{A}} \sqrt{4\sqrt{F(W_{P,B,N}^{(i)})}} \leq 2\sum_{i\in\mathcal{A}} \sqrt{2^{-N^\beta}} = o\left(2^{-\frac{1}{2}N^\beta}\right).
\end{aligned}$$

The first inequality is from Proposition 1 in Ref. [3]. The second inequality follows from a fidelity uncertainty relation

$$\sqrt{F(W_{A,E,N}^{(i)})} + 2\sqrt{F(W_{P,B,N}^{(i)})} \geq 1, \tag{13}$$

proved in Appendix C of Ref. [15]. The fourth inequality follows from the definition of the set $\mathcal{A}$. ∎

III. Vanishing Secret-Key Rate

The rate of secret key required by our polar coding scheme vanishes whenever the quantum wiretap channel $\mathcal{N}^{A'\to BE}$ is *degradable*, meaning that there exists some degrading map $\mathcal{D}^{B\to E}$ that allows the legitimate receiver to simulate the output of the wiretapper: $\mathcal{D}^{B\to E}\circ\mathcal{N}^{A'\to B}=\mathcal{N}^{A'\to E}$. This condition holds for many channels of interest such as the amplitude damping channel and the dephasing channel.

The argument proceeds similarly to the argument in Ref. [15]. The argument there demonstrates that the entanglement consumption rate of a quantum polar code vanishes for degradable channels (this argument in turn is similar to the original argument in Ref. [1]). We merely highlight the argument and point the interested reader to Appendix C of Ref. [15] for the details. From the fidelity uncertainty relation in (13), we know that the phase-good channels to Bob should be amplitude-"very bad" to Eve, in the sense that

$$\sqrt{F(W^{(i)}_{P,B,N})}<2^{-N^\beta}\implies\sqrt{F(W^{(i)}_{A,E,N})}>1-2\cdot 2^{-N^\beta}.$$

From degradability, we also know that the doubly-bad channels in B are amplitude-bad channels to Eve (if they are bad for Bob, then they are worse for Eve.). These observations imply that the phase-good channels to Bob, the doubly-bad channels to Bob, and the amplitude-good channels to Eve are disjoint sets. From Theorem 1, the sum rate of the phase-good channels to Bob and the amplitude-good channels to Eve is equal to $I(W_{P,B})+I(W_{A,E})=1$ as $N\to\infty$. Thus, the rate of the doubly-bad set is zero in the same limit.

The theorem below provides another sufficient condition for when our private polar code has a vanishing secret key rate. The argument proceeds along the lines given in Section 7.1 of Ref. [6], with the fidelity replacing the Bhattacharya parameter. We provide a proof in Appendix B for completeness.

Theorem 3: If the following inequality holds, then the private polar coding scheme has a vanishing secret key rate:

$$\sqrt{F(W_{A,B})}+\sqrt{F(W_{P,B})}<1.$$

$F(W_{A,B})$ and $F(W_{P,B})$ are the fidelities of the amplitude channel in (1) and the phase channel in (5), respectively.

It is our suspicion that channels satisfying the above condition do not require any secret key at all, but we have not been able to prove it (we discuss this point further in Appendix B). We note that the above theorem provides a similar sufficient condition for the quantum polar codes from Ref. [15] to determine if the codes there have a vanishing rate of entanglement consumption.

In Appendix C, we compute $\sqrt{F(W_{A,B})}+\sqrt{F(W_{P,B})}$ for several example channels, including the binary symmetric wiretap channel from Ref. [1], the erasure wiretap channel, and the amplitude damping channel. We find that the secret key rate vanishes for a wide range of interesting parameters.

IV. Conclusion

Building on the general approach from Ref. [13], we have constructed a polar coding scheme for private classical communication over a quantum wiretap channel which achieves the symmetric private information rate. By considering the associated classical amplitude and phase channels of the wiretap channel, we are able to demonstrate that the scheme is both reliable and strongly secure. Indeed, the reliability of non-private polar coding is sufficient, as the strong security of the private protocol follows from the reliability of the phase channel coding. Additionally, we have shown that the secret-key consumption rate vanishes for all degradable quantum wiretap channels or channels satisfying a simple fidelity criterion. As classical wiretap channels are a special form of quantum wiretap channels, all of our results apply to them as well. It would be interesting to find an argument ensuring reliability and strong security of the scheme which relies only on a classical description of the wiretap channel. Further important open questions include whether there is an efficient implementation of the quantum successive cancellation decoder used here, if there is a fast algorithm for determining the good and bad channels, and if the condition in Theorem 3 implies that the codes require no secret key at all.

We thank Frederic Dupuis for useful feedback on Theorem 3. MMW acknowledges support from the Centre de Recherches Mathématiques, and JMR acknowledges support from the Swiss National Science Foundation and the European Research Council.

References

[1] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, October 2011, arXiv:1001.0210.

[2] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[3] M. M. Wilde and S. Guha, "Polar codes for classical-quantum channels," September 2011, arXiv:1109.2591.

[4] ——, "Polar codes for degradable quantum channels," September 2011, arXiv:1109.5346.

[5] J. M. Renes and J.-C. Boileau, "Conjectured strong complementary information tradeoff," *Phys. Rev. Lett.*, vol. 103, p. 020402, July 2009.

[6] J. M. Renes, F. Dupuis, and R. Renner, "Efficient quantum polar coding," September 2011, arXiv:1109.3195.

[7] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, no. 1, p. 44, January 2005, arXiv:quant-ph/0304127.

[8] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, no. 4, pp. 318–336, October 2004.

[9] M. M. Wilde, *From Classical to Quantum Shannon Theory*, June 2011, arXiv:1106.1445.

[10] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "Secure key from bound entanglement," *Physical Review Letters*, vol. 94, p. 160502, April 2005.

[11] ——, "General paradigm for distilling classical key from quantum states," *IEEE Transactions on Information Theory*, vol. 55, pp. 1898–1929, 2009.

[12] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[13] J. M. Renes and J.-C. Boileau, "Physical underpinnings of privacy," *Physical Review A*, vol. 78, p. 032335, September 2008.

[14] E. Arikan and E. Telatar, "On the rate of channel polarization," in *Proceedings of the 2009 International Symposium on Information Theory*, Seoul, Korea, June 2009, pp. 1493–1495, arXiv:0807.3806.

[15] M. M. Wilde and J. M. Renes, "Quantum polar codes for arbitrary channels," January 2012, arXiv:1201.2906.

APPENDIX A
CLASSICAL WIRETAP CHANNELS AS QUANTUM WIRETAP CHANNELS

Suppose that $p(y,z|x)$ is a classical wiretap channel such that x is the input and y and z are the outputs for the legitimate receiver and the wiretapper, respectively. Then we can embed the random variables X, Y, and Z into quantum systems, so that the resulting wiretap channel has the following action on an arbitrary input state ρ:

$$\mathcal{N}_{\mathrm{C}}^{A'\to BE}(\rho) \equiv \sum_{x,y,z} \langle x|\rho|x\rangle \; p(y,z|x)\, |y\rangle^B \otimes |z\rangle^E \langle y|^B \otimes \langle z|^E . \tag{14}$$

The physical interpretation of the above channel is that it first *measures* the input system in the orthonormal basis $\{|x\rangle\langle x|\}$ (ensuring that the input is effectively classical) and *prepares* the classical states $|y\rangle^B$ and $|z\rangle^E$ for Bob and Eve with probability $p(y,z|x)$. One can check that the Kraus operators [9] for this classical channel are

$$\left\{ \sqrt{p(y,z|x)} \left(|y\rangle^B \otimes |z\rangle^E \right) \langle x|^{A'} \right\}_{x,y,z}.$$

Thus, by a standard construction [9], an isometric extension of this classical wiretap channel acts as follows on a pure state input $|\psi\rangle$:

$$U_{\mathcal{N}_{\mathrm{C}}}^{A'\to BES_2} |\psi\rangle = \sum_{x,y,z} \sqrt{p(y,z|x)} \left(|y\rangle^B \otimes |z\rangle^E \right) \langle x|^{A'} |\psi\rangle \otimes |x,y,z\rangle^{S_2},$$

so that tracing over system S_2 recovers the action of the original channel in (14).[1]

APPENDIX B
PROOF OF THEOREM 3

As described in Section II-B, one can prove that channel polarization takes hold by considering the channel splitting and combining process as a random birth process $\{W_n : n \geq 0\}$ (with the channel choice picked by some IID Bernoulli process $\{B_n : n \geq 1\}$ and setting $W_0 = W$). One can then consider the induced birth process

$$\{F_n : n \geq 0\} \equiv \{\sqrt{F(W_n)} : n \geq 0\}$$

for the fidelity channel parameter. The inequalities (26-27) from Ref. [3] (an extension of Arikan's inequalities [2]) demonstrate that the following extremal process $\{F'_n : n \geq 0\}$ bounds the actual channel process $\{F_n : n \geq 0\}$:

$$F'_{n+1} = \begin{cases} F'^2_n & \text{if} \quad B_n = 0 \\ 2F'_n - F'^2_n & \text{if} \quad B_n = 1 \end{cases},$$

a relation which can be written more symmetrically as

$$\begin{aligned} F'_{n+1} &= F'^2_n && \text{if} \quad B_n = 0, \\ 1 - F'_{n+1} &= (1 - F'_n)^2 && \text{if} \quad B_n = 1. \end{aligned} \tag{15}$$

From now on, we make abbreviations such as $\{F_n\} = \{F_n : n \geq 0\}$ in order to simplify the notation.

The extremal process above has the nice property [14, Observation 4 (ii)] (see the arXiv version) that for every realization $\{b_n\}$ of the process $\{B_n\}$ (and thus for every realization $\{f'_n\}$ of $\{F'_n\}$) there exists a particular initial threshold value $F'_{\text{th}}(\{b_n\})$ such that either

$$\lim_{n\to\infty} f'_n = 0 \text{ if } F'_0 < F'_{\text{th}}(\{b_n\}),$$

or

$$\lim_{n\to\infty} f'_n = 1 \text{ if } F'_0 \geq F'_{\text{th}}(\{b_n\}).$$

(Note that F'_0 is deterministic and is the initial value of the process.)

We can denote the respective fidelity processes for the amplitude and phase channels in our coding scheme as $\{F^A_n\}$ and $\{F^P_n\}$ and the respective random birth processes as $\{B^A_n\}$ and $\{B^P_n\}$. Also, let $\{F^{A\prime}_n\}$ and $\{F^{P\prime}_n\}$ denote the corresponding extremal processes. The important observation made in Ref. [6] is that the process $\{F^P_n\}$ makes the opposite choice of channel at each step of the birth process because the phase encoder is the reverse of the amplitude encoder. That is, it holds for every n and for every realization $\{b^A_n\}$ and $\{b^P_n\}$ that

$$b^P_n = 1 - b^A_n.$$

[1]The square root of a probability might seem strange at first glance when appearing in an evolution, but it is in fact quite natural in quantum information theory, being interpreted physically as a probability amplitude.

Thus, we can write $B_n^P = 1 - B_n^A$, so that B_n^P is completely determined by B_n^A. The extremal amplitude channel process $\left\{F_n^{A\prime}\right\}$ is already of the form in (15), and we can consider the extremal phase process as $\left\{1 - F_n^{P\prime}\right\}$ in order for it to have this same form. Thus, a realization $\{f_n^{A'}\}$ of the extremal amplitude channel process $\left\{F_n^{A\prime}\right\}$ converges to one if

$$F_0^{A\prime} \geq F'_{\text{th}}(\{b_n^A\}),$$

and a realization $\{1 - f_n^{P'}\}$ of the extremal phase process $\left\{1 - F_n^{P\prime}\right\}$ converges to zero if

$$1 - F_0^{P\prime} < F'_{\text{th}}(\{b_n^A\}),$$

implying that $\left\{f_n^{P\prime}\right\}$ converges to one if

$$F_0^{P\prime} > 1 - F'_{\text{th}}(\{b_n^A\}).$$

Thus, the sum process $\left\{F_n^{A\prime} + F_n^{P\prime}\right\}$ converges to two if

$$\begin{aligned} F_0^{A\prime} + F_0^{P\prime} &\geq F'_{\text{th}}(\{b_n^A\}) + 1 - F'_{\text{th}}(\{b_n^A\}) \\ &= 1. \end{aligned} \tag{16}$$

The above bound is a *universal*, sufficient lower bound for the sum process to converge to two, that holds regardless of the threshold value $F'_{\text{th}}(\{b_n^A\})$ for a particular realization $\{b_n^A\}$. It follows that a given realization $\left\{f_n^A + f_n^P\right\}$ of the actual sum process $\left\{F_n^A + F_n^P\right\}$ can only converge to two when (16) holds because we set $F_0^{A'} = F_0^A$ and the extremal process bounds the actual process (note that some realizations might converge to one or zero as well). If a realization $\left\{f_n^A + f_n^P\right\}$ of the sum process $\left\{F_n^A + F_n^P\right\}$ converges to two, then this implies that the set $\mathcal{B}$ is non-empty, i.e., the code will require some secret key bits. So, if the condition in the statement of the theorem holds, no realization of the sum process can ever converge to two, and the code will not require any secret key bits.

The above argument only holds in the asymptotic limit of many recursions of the encoding such that the channel polarization effect takes hold (where all synthesized channels are polarized to be completely perfect or useless). That is, the argument does not apply whenever there is a finite number of recursions—in this case, if the number of recursions is large enough, then a large fraction of synthesized channels polarize according to some tolerance, but there is always a small fraction that have not polarized. Thus, we can only conclude that the above proof applies in the limit of many recursions and that the rate of secret key consumption vanishes in this limit. It is an open question to adapt the above argument to the finite case, but we suspect that some form of it holds in this regime.

APPENDIX C
EXAMPLE CHANNELS

In this appendix, we evaluate the condition from Theorem 3 for several examples, including the independent binary symmetric wiretap channel model from Ref. [1], the erasure wiretap channel, and the amplitude damping channel. For many of these cases, we find that the resulting polar codes have a vanishing secret key rate for a wide range of parameters.

A. Binary Symmetric Wiretap Channel

Suppose that the channel to Bob is a binary symmetric channel with flip probability p_B and the channel to Eve is an independent binary symmetric channel with flip probability p_E. The symmetric private information for this channel is equal to

$$(1 - H_2(p_B)) - (1 - H_2(p_E)) = H_2(p_E) - H_2(p_B),$$

which is only positive whenever $p_B < p_E$. The conditional distribution $p(y, z|x)$ for this channel is just

$$p(y, z|x) = (p_B)^{x+y} (1 - p_B)^{x+y+1} (p_E)^{x+z} (1 - p_E)^{x+z+1}, \tag{17}$$

where Alice inputs x, Bob receives output y, Eve receives output z, and $y, z, x \in \{0, 1\}$. Observe that the above channel factorizes as

$$p(y, z|x) = p(y|x)\, p(z|x),$$

where

$$\begin{aligned} p(y|x) &= (p_B)^{x+y} (1 - p_B)^{x+y+1}, \\ p(z|x) &= (p_E)^{x+z} (1 - p_E)^{x+z+1}. \end{aligned}$$

Since the amplitude channel to Bob in this case is just a binary symmetric channel with flip probability p_B, the root fidelity $\sqrt{F(W_{A,B})}$ just reduces to the classical Bhattacharya parameter:

$$\sqrt{F(W_{A,B})} = 2\sqrt{p_B (1 - p_B)}.$$

We now need to compute the fidelity for the phase channel to Bob. Since Alice inputs classical states $|z\rangle$ to the amplitude channel, the states $|\psi_z\rangle$ in (4) are just equal to $|z\rangle$ (there is no shield system S_1). This implies that the quantum input for the phase channel is of the form

$$Z^{x'} \frac{1}{\sqrt{2}} \sum_{z'} |z'\rangle^C |z'\rangle^{A'} = \frac{1}{\sqrt{2}} \sum_{z'} (-1)^{x' \cdot z'} |z'\rangle^C |z'\rangle^{A'},$$

if x' is the input bit. The isometric extension of this classical wiretap channel is then just

$$\sum_{x,y,z} \sqrt{p(y,z|x)} \left(|y\rangle^B \otimes |z\rangle^E \right) \langle x|^{A'} \otimes |x,y,z\rangle^{S_2},$$

with $p(y,z|x)$ given by (17), so that the action on the above input state is

$$\begin{aligned} x' \rightarrow & \frac{1}{\sqrt{2}} \sum_{x,y,z,z'} (-1)^{x' \cdot z'} \sqrt{p(y,z|x)} |y\rangle^B |z\rangle^E |z'\rangle^C \langle x|z'\rangle^{A'} \otimes |x,y,z\rangle^{S_2} \\ = & \frac{1}{\sqrt{2}} \sum_{x,y,z} (-1)^{x' \cdot x} \sqrt{p(y,z|x)} |y\rangle^B |z\rangle^E |x\rangle^C \otimes |x,y,z\rangle^{S_2}. \end{aligned}$$

To simplify things, we will write $p(x) = 1/2$, giving

$$x' \rightarrow \sum_{x,y,z} (-1)^{x' \cdot x} \sqrt{p(y,z|x)\, p(x)} |y\rangle^B |z\rangle^E |x\rangle^C \otimes |x,y,z\rangle^{S_2}$$

Tracing over the E system then gives the phase channel to Bob:

$$\begin{aligned} & \text{Tr}_E \left\{ \sum_{x,y,z,x'',y'',z''} (-1)^{x' \cdot x} (-1)^{x' \cdot x''} \sqrt{p(y,z|x)\, p(x)\, p(y'',z''|x'')\, p(x'')} |y\rangle \langle y''|^B |z\rangle \langle z''|^E |x\rangle \langle x''|^C \otimes |x,y,z\rangle \langle x'',y'',z''|^{S_2} \right\} \\ = & \sum_{x,y,z,x'',y''} (-1)^{x' \cdot (x+x'')} \sqrt{p(y,z|x)\, p(x)\, p(y'',z|x'')\, p(x'')} |y\rangle \langle y''|^B \otimes |x\rangle \langle x''|^C \otimes |x,y,z\rangle \langle x'',y'',z|^{S_2} \\ = & \sum_{x,y,z,x'',y''} (-1)^{x' \cdot (x+x'')} \sqrt{p(y|x)\, p(z|x)\, p(x)\, p(y''|x'')\, p(z|x'')\, p(x'')} |y\rangle \langle y''|^B \otimes |x\rangle \langle x''|^C \otimes |x,y,z\rangle \langle x'',y'',z|^{S_2} \\ = & \sum_{x,y,z,x'',y''} (-1)^{x' \cdot (x+x'')} \sqrt{p(y|x)\, p(x|z)\, p(z)\, p(y''|x'')\, p(x''|z)\, p(z)} |y\rangle \langle y''|^B \otimes |x\rangle \langle x''|^C \otimes |x,y,z\rangle \langle x'',y'',z|^{S_2} \end{aligned}$$

We can then factorize the above state as follows:

$$\omega_{x'}^{BCS_X S_Y S_Z} \equiv \sum_z p(z) |\chi_{z,x'}\rangle \langle \chi_{z,x'}|^{BCS_X S_Y} \otimes |z\rangle \langle z|^{S_Z},$$

where

$$|\chi_{z,x'}\rangle^{BCS_X S_Y} \equiv \frac{1}{\sqrt{2}} \sum_{x,y} (-1)^{x' \cdot x} \sqrt{p(y|x)\, p(x|z)} |y\rangle^B |x\rangle^C |x\rangle^{S_X} |y\rangle^{S_Y}.$$

Noting that $p(z) = 1/2$, we now compute the fidelity $\sqrt{F(W_{P,B})}$ as

$$\begin{aligned} \sqrt{F(W_{P,B})} &= \sqrt{F\left(\omega_0^{BCS_X S_Y S_Z}, \omega_1^{BCS_X S_Y S_Z}\right)} \\ &= \sum_z \frac{1}{2} \sqrt{F(\chi_{z,0}, \chi_{z,1})} \\ &= \sum_z \frac{1}{2} |\langle \chi_{z,0} | \chi_{z,1} \rangle| \\ &= |p_E - 1/2|, \end{aligned}$$

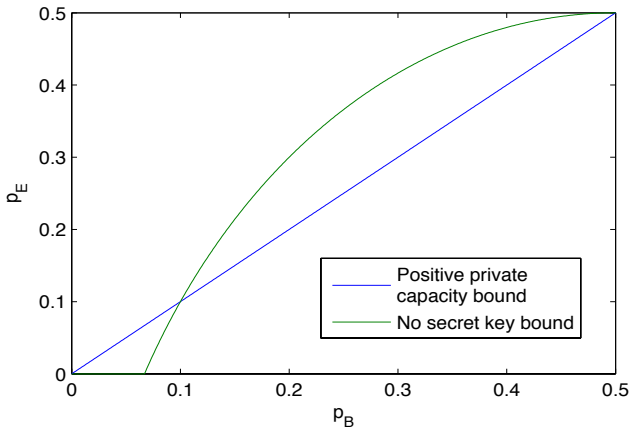

Fig. 1. The parameters p_B and p_E correspond to bit flip probabilities in the binary symmetric wiretap channel. Below the blue line is the region where the symmetric private information is positive. Below the green line is the region for when the secret key rate of the code vanishes according to Theorem 3. The result is that the polar code has a vanishing secret key rate for a wide range of interesting parameters p_B and p_E.

where the last line follows from

$$\begin{aligned}
|\langle\chi_{z,0}|\chi_{z,1}\rangle| &= \frac{1}{2}\left|\sum_{x,y,x'',y''}(-1)^x\sqrt{p\left(y''|x''\right)p\left(x''|z\right)p\left(y|x\right)p\left(x|z\right)}\left\langle y''\right|\left|y\right\rangle^B\left\langle x''\right|\left|x\right\rangle^C\left\langle x''\right|\left|x\right\rangle^{S_X}\left\langle y''\right|\left|y\right\rangle^{S_Y}\right| \\
&= \frac{1}{2}\left|\sum_{x,y}(-1)^x p\left(y|x\right)p\left(x|z\right)\right| \\
&= \frac{1}{2}\left|\sum_{x}(-1)^x p\left(x|z\right)\right| \\
&= \frac{1}{2}\left|\sum_{x}(-1)^x \left(p_E\right)^{x+z}\left(1-p_E\right)^{x+z+1}\right| \\
&= \left|p_E - 1/2\right|.
\end{aligned}$$

The relation $p\left(x|z\right) = p\left(z|x\right)$ follows because $p\left(x\right) = p\left(z\right) = 1/2$.

Thus, from Theorem 3, the sufficient condition for the wiretap channel in (17) to have a vanishing secret key rate is just

$$2\sqrt{p_B\left(1-p_B\right)} + \left|p_E - 1/2\right| < 1.$$

If we assume that $p_E < 1/2$, then this reduces to

$$2\sqrt{p_B\left(1-p_B\right)} < 1/2 + p_E.$$

Figure 1 provides a plot of two bounds: a bound for when the symmetric private information is positive and bound for when the polar code has a vanishing secret key rate. We find that the secret key rate vanishes for a wide range of parameters.

B. Erasure Channel

An erasure channel transmits the input bit with probability $1-\epsilon$ and provides an erasure symbol e to the receiver (different from 0 or 1) with probability ϵ. A simple model for a channel to the wiretapper is to give the input bit to the wiretapper whenever the receiver gets the erasure symbol (thus, the channel to the wiretapper is an erasure channel with erasure probability $1-\epsilon$).

It turns out that this model is equivalent to the quantum erasure channel:

$$\rho \to \left(1-\epsilon\right)\rho + \epsilon\left|e\right\rangle\left\langle e\right|,$$

for which it is well known that the complementary channel is just

$$\rho \to \epsilon\rho + \left(1-\epsilon\right)\left|e\right\rangle\left\langle e\right|,$$

so that this channel is equivalent to the wiretap channel mentioned above. Both the quantum and private capacities of this channel are equal to $1 - 2\epsilon$.

The amplitude channel to Bob is just an erasure channel with erasure probability ϵ. We now consider the phase channel to Bob:

$$x \to \mathcal{N}\left(Z^x \left|\Phi\right\rangle \left\langle\Phi\right| Z^x\right) = \epsilon Z^x \left|\Phi\right\rangle \left\langle\Phi\right| Z^x + (1-\epsilon)\,\pi \otimes \left|e\right\rangle \left\langle e\right|,$$

where π is the maximally mixed state. It is clear that the above channel is also just an erasure channel with erasure probability ϵ because Bob can perform the measurement $\{\left|0\right\rangle \left\langle 0\right| + \left|1\right\rangle \left\langle 1\right|, \left|e\right\rangle \left\langle e\right|\}$ on the second qubit to determine if he received the state. If he does receive it, he can then perform a Bell measurement to retrieve the bit x.

Since the root fidelity of an erasure channel is just ϵ, the condition from Theorem 3 for vanishing secret key rate just reduces to

$$2\epsilon < 1,$$

which is satisfied for all erasure probabilities ϵ for which the private information is positive.

C. Amplitude Damping Channel

The last example of a channel that we study is the amplitude damping channel. This channel models photon loss when transmitting a state in the zero or single-photon subspace over a pure-loss bosonic channel (a beamsplitter with transmissivity η). The Kraus operators for this channel are

$$\begin{aligned} A_0 &\equiv \sqrt{1-\eta}\left|0\right\rangle \left\langle 1\right|, \\ A_1 &\equiv \left|0\right\rangle \left\langle 0\right| + \sqrt{\eta}\left|1\right\rangle \left\langle 1\right|, \end{aligned}$$

so that the evolution of an input qubit is

$$\rho \to A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger.$$

This channel has a positive private capacity whenever $\eta > 1/2$. If $\eta \leq 1/2$, then the majority of the output is going to the wiretapper (or the environment of the channel) and so there is not any positive private capacity for this parameter range.

The amplitude channel to Bob is

$$\begin{aligned} 0 &\to A_0 \left|0\right\rangle \left\langle 0\right| A_0^\dagger + A_1 \left|0\right\rangle \left\langle 0\right| A_1^\dagger = \left|0\right\rangle \left\langle 0\right|, \\ 1 &\to A_0 \left|1\right\rangle \left\langle 1\right| A_0^\dagger + A_1 \left|1\right\rangle \left\langle 1\right| A_1^\dagger = (1-\eta)\left|0\right\rangle \left\langle 0\right| + \eta \left|1\right\rangle \left\langle 1\right|. \end{aligned}$$

Thus, the fidelity for this amplitude channel is $\sqrt{1-\eta}$.

Now consider the phase channel:

$$x \to \mathcal{N}\left(Z^x \left|\Phi\right\rangle \left\langle\Phi\right| Z^x\right),$$

where $\left|\Phi\right\rangle$ is the Bell state. Analyzing for this case gives

$$(1-\eta)\left|0\right\rangle \left\langle 1\right| \left(Z^x \left|\Phi\right\rangle \left\langle\Phi\right| Z^x\right) \left|1\right\rangle \left\langle 0\right| + \left(\left|0\right\rangle \left\langle 0\right| + \sqrt{1-\gamma}\left|1\right\rangle \left\langle 1\right|\right) \left(Z^x \left|\Phi\right\rangle \left\langle\Phi\right| Z^x\right) \left(\left|0\right\rangle \left\langle 0\right| + \sqrt{1-\gamma}\left|1\right\rangle \left\langle 1\right|\right)$$

We handle the first term:

$$\begin{aligned} (1-\eta)\left|0\right\rangle \left\langle 1\right| \left(Z^x \left|\Phi\right\rangle \left\langle\Phi\right| Z^x\right) \left|1\right\rangle \left\langle 0\right| &= \frac{1-\eta}{2}\left|0\right\rangle \left\langle 1\right| \left(\left|00\right\rangle \left\langle 00\right| + (-1)^x \left|11\right\rangle \left\langle 00\right| + (-1)^x \left|00\right\rangle \left\langle 11\right| + \left|11\right\rangle \left\langle 11\right|\right) \left|1\right\rangle \left\langle 0\right| \\ &= \frac{1-\eta}{2}\left|10\right\rangle \left\langle 10\right| \end{aligned}$$

We handle the second term:

$$\begin{aligned} &\left(\left|0\right\rangle \left\langle 0\right| + \sqrt{\eta}\left|1\right\rangle \left\langle 1\right|\right) \left(Z^x \left|\Phi\right\rangle \left\langle\Phi\right| Z^x\right) \left(\left|0\right\rangle \left\langle 0\right| + \sqrt{\eta}\left|1\right\rangle \left\langle 1\right|\right) \\ &= \frac{1}{2}\left(\left|0\right\rangle \left\langle 0\right| + \sqrt{\eta}\left|1\right\rangle \left\langle 1\right|\right) \left(\left|00\right\rangle \left\langle 00\right| + (-1)^x \left|11\right\rangle \left\langle 00\right| + (-1)^x \left|00\right\rangle \left\langle 11\right| + \left|11\right\rangle \left\langle 11\right|\right) \left(\left|0\right\rangle \left\langle 0\right| + \sqrt{\eta}\left|1\right\rangle \left\langle 1\right|\right) \\ &= \frac{1}{2}\left(\left|00\right\rangle \left\langle 00\right| + (-1)^x \sqrt{\eta}\left|11\right\rangle \left\langle 00\right| + (-1)^x \left|00\right\rangle \left\langle 11\right| + \sqrt{\eta}\left|11\right\rangle \left\langle 11\right|\right) \left(\left|0\right\rangle \left\langle 0\right| + \sqrt{\eta}\left|1\right\rangle \left\langle 1\right|\right) \\ &= \frac{1}{2}\left(\left|00\right\rangle \left\langle 00\right| + (-1)^x \sqrt{\eta}\left|11\right\rangle \left\langle 00\right| + (-1)^x \sqrt{\eta}\left|00\right\rangle \left\langle 11\right| + \eta\left|11\right\rangle \left\langle 11\right|\right) \end{aligned}$$

Adding the two terms gives

$$\frac{1}{2}\left(\left|00\right\rangle \left\langle 00\right| + (-1)^x \sqrt{\eta}\left|11\right\rangle \left\langle 00\right| + (-1)^x \sqrt{\eta}\left|00\right\rangle \left\langle 11\right| + \eta\left|11\right\rangle \left\langle 11\right|\right) + \frac{1-\eta}{2}\left|10\right\rangle \left\langle 10\right|$$

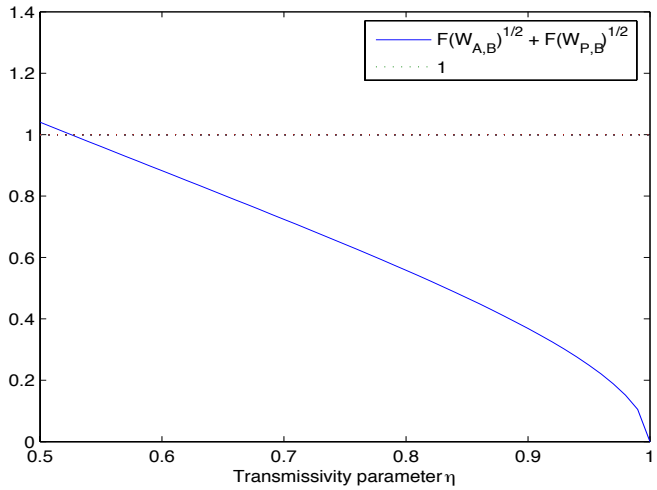

Fig. 2. A comparison of the quantity $\sqrt{F(W_{A,B})} + \sqrt{F(W_{P,B})}$ from Theorem 3 and 1 for various transmissivities η of the amplitude damping channel. The result is that a polar code has a vanishing secret key rate for most η.

which has the following matrix representation in the computational basis:

$$\begin{bmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2}(-1)^x\sqrt{\eta} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1-\eta}{2} & 0 \\ \frac{1}{2}(-1)^x\sqrt{\eta} & 0 & 0 & \frac{\eta}{2} \end{bmatrix}.$$

We numerically compute the fidelity for the phase channel, and the plot in Figure 2 shows all of the damping parameters which meet the condition from Theorem 3. The result is that the polar has a vanishing secret key rate for most transmissivities η.